



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER TO: Joint Interoperability Test Command (JTE)

22 Aug 12

SUBJECT: Special Interoperability Test Certification of the Cisco Nexus 7000 series Switch Release NX OS 6.0(1).

- References:
- (a) Department of Defense Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004.
 - (b) Chairman, Joint Chiefs of Staff Instruction 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008.
 - (c) through (e), see Enclosure 1.

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability (IO) test certification.

2. The Cisco N7K-C7010 Switch Release NX OS 6.0(1) is hereinafter referred to as the system under test (SUT). The SUT meets all of its critical IO requirements and is certified for joint use within the Defense Information System Network (DISN) as an Assured Services Local Area Network (ASLAN) Core, Distribution, and Layer 2/Layer 3 Access switch. However, there are restrictions on the SUT functioning as a certified Core or Distribution switch. These restrictions are discussed in the following tables within this memorandum. The SUT is certified as interoperable for joint use with other ASLAN components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10/100/1000BaseT and 1000BaseX for access, 1000BaseT and 1000/10000BaseX for uplink. All of these interfaces were tested with the exception of the 10BaseT interface. JITC analysis determined that the 10BaseT interface is a low risk for certification based on the vendor's Letter of Compliance (LoC) to comply with the Institute of Electrical and Electronics Engineers (IEEE) 802.3i standard and the testing data collected at all other data rates. The SUT meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). The Cisco N7K-C7018 and N7K-C7009 switches employ the same software and similar hardware as the SUT. JITC analysis determined these systems to be functionally identical to the SUT for interoperability certification purposes, and they are also certified for joint use.

The SUT is certified to support Assured Services within an ASLAN. If a component meets the minimum requirements for deployment in an ASLAN, it also meets the lesser requirements for deployment in a non-ASLAN. Non-ASLANs are "commercial grade" and provide support to Command and Control (C2) (ROUTINE only calls) (C2(R)) or non-C2 voice subscribers. When deployed in a non-ASLAN, the SUT may also be used to receive all levels of precedence, but is limited to supporting calls that are originated at ROUTINE precedence only. Non-ASLANs do

not meet the availability or redundancy requirements for C2 or Special C2 users and therefore are not authorized to support precedence calls originated above ROUTINE.

Testing of the SUT did not include video services or data applications; however, simulated video traffic, preferred data, and best effort data were generated during testing to determine the SUT's ability to prioritize and properly queue voice media and signaling traffic. No other configurations, features, or functions, except those cited within this document, are certified by JITC. This certification expires upon changes that affect IO but no later than three years from the date of the UC APL memorandum.

3. This finding is based on IO testing conducted by the United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), review of the vendor's LoC, DISA adjudication of open test discrepancy reports (TDRs), and the DISA Certifying Authority (CA) Recommendation. The IO testing was conducted by the USAISEC TIC, Fort Huachuca, Arizona, from 13 February through 16 March 2012. Review of the vendor's LoC was completed on 8 May 2012. The DISA adjudication of outstanding TDRs was completed on 10 July 2012. The DISA CA provided a positive recommendation on 8 June 2012, based on the security testing completed by USAISEC TIC-led information assurance (IA) test teams. Those test results are published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations.

4. Table 1 provides a UC APL product summary. Table 2 provides the SUT interface IO status and Table 3 provides the Capability Requirements (CRs) and Functional Requirements (FRs) status. The threshold CRs/FRs for ASLAN components are established by Section 5.3.a of Reference (c) and were used to evaluate the IO of the SUT. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

Table 1. UC APL Product Summary

Component ¹	Release	Sub-Component ¹	Certification Applicability		
			Core	Distribution	Access
<u>Cisco N7K-C7010</u>	NX OS 6.0(1)	<u>N7K-SUP1, N7K-C7010-FAB-2, N7K-M148GT-11, N7K-M148GS-11, N7K-M148GS-11L, N7K-M108X2-12L, N7K-M132XP-12L^{2,3}, N7K-F132XP-15, N7K-F248XP-25, N7K-C7009-FAB-2, N7K-C7018-FAB-2, N7K-M148GT-11L</u>	Yes	Yes	Yes
Cisco N7K-C7018		The following modules were certified during previous ASLAN certifications and recertified based on technology maturity per UCR 2008, Change 3, Section 4.4.2:			
Cisco N7K-C7009		N7K-M132XP-12 ^{2,3} , N7K-C7010-FAB-1, N7K-C7018-FAB-1			

Table 1. UC APL Product Summary (continued)

NOTE: 1. Components bolded and underlined> were tested by the USAISEC TIC. The other components in the family series were not tested; however, they utilize the same OS software and similar hardware. JITC analysis determined them to be functionally identical for IO certification purposes and they are also certified for joint use. 2. The SUT complies with the Non-blocking requirement in the Performance Parameters IAW UCR 2008, Change 3, Section 5.3.1.3, Paragraph 1 as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the “Performance Mode” (see deployment guide) with the following modules: N7K-M132XP-12L and N7K-M132XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the “Default Mode” or “Oversubscription Mode” would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the “Default” or “Oversubscription” mode of operation. 3. The SUT complies with the QoS blocking factor features IAW the UCR 2008, Change 3, Section 5.3.1.3.6, Paragraph 5b as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the “Performance Mode” (see deployment guide) with the following modules: N7K-M132-XP-12L and N7K-M132-XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the “Default Mode” or “Oversubscription Mode” would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the “Default” or “Oversubscription” mode of operation.		
LEGEND: APL Approved Products List ASLAN Assured Services Local Area Network DISA Defense Information Systems Agency IAW In Accordance With IO Interoperability JITC Joint Interoperability Test Command NX Nexus		
OS Operating System QoS Quality of Service SUT System Under Test TIC Technology Integration Center UC Unified Capabilities UCR Unified Capabilities Requirements USAISEC U.S. Army Information Systems Engineering Command		

Table 2. SUT Interface Interoperability Status

Interface	Applicability			UCR 2008, Change 3 Reference	Threshold CR/FR ¹	Status	Remarks
	Co	D	A				
Serial	C	C	C	5.3.1.3.9	1-4	Certified	The SUT met the CRs and FRs with the following standard: EIA-232.
10Base-X	C	C	C ²	5.3.1.3.1	1-6	Certified ³	The SUT met CRs and FRs with the following IEEE standard: 802.3i (10BaseT).
100Base-X	R	R	C ²	5.3.1.3.1	1-6	Certified	The SUT met CRs and FRs with the following IEEE standard: 802.3u (100BaseT).
1000Base-X	R	R	C ²	5.3.1.3.1	1-6	Certified	The SUT met CR and FRs with the following IEEE standards: 802.3ab (1000BaseT), 802.3z (1000Base-SX, 1000Base-LX).
10000Base-X	C	C	C	5.3.1.3.1	1-6	Certified	The SUT met CRs and FRs with the following IEEE standard: 802.3ae (10GBase-SR, 10GBase-LR).
802.11a	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.11b	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.11g	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.11n	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.16	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A

Table 2. SUT Interface Interoperability Status (continued)

NOTES:			
1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.			
2. Core and Distribution products must minimally support 100Base-X (802.3u) and 1000Base-X (802.3z). Access products must minimally support one of the following standards: 802.3i (10BaseT), 802.3j (10BaseF), 802.3u (100BaseT/F), 802.3z (1000BaseF), or 802.3ab (1000BaseT). Other rates and standards may be provided as conditional interfaces.			
3. The USAISEC TIC tested all these interfaces with the exception of the 10BaseT interface. JITC analysis determined that the 10BaseT interface is a low risk for certification based on the vendor's LoC to the IEEE 802.3i and the testing data collected at all other data rates.			
4. The SUT does not support this interface. This interface is not required for a Core, Distribution, or Access switch.			
LEGEND:			
802.3ab	1000BaseT Gbps Ethernet Over Twisted Pair at 1Gbps (125 Mbps)	A	Access
802.3ae	10 Gbps Ethernet	C	Conditional
802.3i	10BaseT Mbps Over Twisted Pair	Co	Core
802.3j	10 Mbps Over Fiber	CR	Capability Requirement
802.3u	Standard for Carrier Sense Multiple Access with Collision Detection at 100 Mbps	D	Distribution
802.3z	Gigabit Ethernet Standard	EIA	Electronic Industries Alliance
802.11/16	IEEE Wireless Standards	EIA-232	Standard for Defining the Mechanical and Electrical Characteristics for Connecting Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE)
10BaseF	10 Mbps Ethernet Over Fiber		Data Communications Devices
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	FR	Functional Requirement
10Base-X	10 Mbps Ethernet Over Fiber or Copper	Gbps	Gigabits Per Second
100BaseF	100 Mbps Ethernet Over Fiber	ID	Identification
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IEEE	Institute of Electrical and Electronics Engineers
100Base-X	100 Mbps Ethernet Over Fiber or Copper	JITC	Joint Interoperability Test Command
1000BaseF	1000 Mbps Ethernet Over Fiber	LoC	Letter of Compliance
1000Base-LX	1000 Mbps Ethernet Over Fiber	LR	Long Range Optics
1000Base-SX	1000 Mbps Ethernet Over Fiber	LX	Single-Mode Fiber Optics
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	Mbps	Megabits Per Second
1000Base-X	1000 Mbps Ethernet Over Fiber or Copper	N/A	Not Applicable
10000Base-X	10000 Mbps Ethernet Over Fiber or Copper	R	Required
10GBase-LR	10000 Mbps Ethernet Over Fiber	SR	Short Range Optics
10GBase-SR	10000 Mbps Ethernet Over Fiber	SX	Multi-Mode Fiber Optics
		SUT	System Under Test
		TIC	Technology Integration Center
		UCR	Unified Capabilities Requirements
		USAISEC	U.S. Army Information Systems Engineering Command

Table 3. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability ¹	UCR 2008, Change 3 Reference	Status	Remarks
1	General Performance Parameters				
	Performance Parameters	Required	5.3.1.3	Partially Met ²	
	Port Interface Rates	Required	5.3.1.3.1	Met	
	Port Parameter Requirements	Required	5.3.1.3.2	Partially Met ³	
	Class of Service Markings	Required	5.3.1.3.3	Met	
	VLAN Capabilities	Required	5.3.1.3.4	Met	
	Protocols	Required	5.3.1.3.5	Partially Met ⁴	
	QoS Features	Required	5.3.1.3.6	Partially Met ⁵	
	Network Monitoring	Required	5.3.1.3.7	Met	
	Security	Required	5.3.1.3.8	Met	
2	E2E Performance Requirements				
	Voice Services	Required	5.3.1.4.1	Met ⁶	
	Video Services	Required	5.3.1.4.2	Met ⁶	
	Data Services	Required	5.3.1.4.3	Met ⁶	
3	NM Requirements				
	Configuration Control	Required	5.3.1.6.1	Met	
	Operational Changes	Required	5.3.1.6.2	Met	
	Performance Monitoring	Required	5.3.1.6.3	Met	
	Alarms	Required	5.3.1.6.4	Met	
	Reporting	Required	5.3.1.6.5	Met	
4	Engineering Requirements				
	Physical Media	Required	5.3.1.7.1	Met ⁷	
	Wireless	Conditional	5.3.1.7.2	Not Tested ⁸	
	Traffic Engineering	Required	5.3.1.7.3	Met ⁷	
	Availability	Required	5.3.1.7.6	Met ⁷	
	Redundancy	Required	5.3.1.7.7	Met ⁷	
5	MPLS				
	MPLS Requirements	Conditional	5.3.1.8.4.1	Not Tested ⁸	
	MPLS VPN Augmentation to VLANs	Conditional	5.3.1.8.4.2	Not Tested ⁸	
6	IPv6 Requirements				
	Product Requirements	Required	5.3.5.4	Partially Met ⁴	

Table 3. SUT CRs and FRs Status (continued)

NOTES:

1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. The SUT does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements.
2. The SUT complies with the Non-blocking requirement in the Performance Parameters IAW UCR 2008, Change 3, Section 5.3.1.3, Paragraph 1 as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the "Performance Mode" (see deployment guide) with the following modules: N7K-M132XP-12L and N7K-M132XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the "Default Mode" or "Oversubscription Mode" would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the "Default" or "Oversubscription" mode of operation.
3. The SUT does not support the following Port Parameter Requirements: Link Layer Discovery – Media Endpoint Discovery IAW ANSI/TIA-1057, and Power over Ethernet IAW 802.3af or 802.3at-2009. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as minor. The Power over Ethernet is not supported because the SUT is designed as a Data Center switch. In addition, DISA determined this requirement will change to "optional" in future UCR documents (e.g. UCR 2013).
4. The SUT does not support the following Protocols RFCs: 2560, 3273, 4552, and 5798. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as minor. DoD sites deploying OSPFv3 should use ACLs to secure OSPF until RFC 4552 is supported.
5. The SUT complies with the QoS blocking factor features IAW UCR 2008, Change 3, Section 5.3.1.3.6, Paragraph 5b as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the "Performance Mode" (see deployment guide) with the following modules: N7K-M132-XP-12L and N7K-M132-XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the "Default Mode" or "Oversubscription Mode" would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the "Default" or "Oversubscription" mode of operation.
6. This requirement was verified and met using simulated voice, video, and data traffic in an operational emulated environment to meet E2E requirements. The SUT must be deployed IAW deployment guide and engineering guidelines in UCR 2008, Change 3, Section 5.3.1.4.
7. This requirement was met with the following stipulations: It is the site's responsibility to configure the SUT in a manner which meets the engineering requirements listed in Section 11.2 d. of Enclosure 2, and that it does not create a single point of failure which could impact more than 96 C2 users.
8. Wireless and MPLS were not tested and are not certified for joint use. Wireless and MPLS are conditional and, therefore, not required for a Core, Distribution, or Access switch.

LEGEND:

802.3af	Power Over Ethernet	IPv6	Internet Protocol Version 6
802.3at-2009	Power Over Ethernet Plus	MPLS	Multiprotocol Label Switching
ACL	Access Control List	NM	Network Management
ANSI	American National Standards Institute	OSPF	Open Shortest Path First
C2	Command and Control	OSPFv3	Open Shortest Path First Version 3
CR	Capability Requirement	POA&M	Plan of Action and Milestones
DISA	Defense Information Systems Agency	QoS	Quality of Service
DoD	Department of Defense	RFC	Request For Comment
E2E	End-to-End	SUT	System Under Test
FR	Functional Requirement	TIA	Telecommunications Industry Association
IAW	In Accordance With	UCR	Unified Capabilities Requirements
ID	Identification	VLAN	Virtual Local Area Network
IPv4	Internet Protocol Version 4	VPN	Virtual Private Network

5. In accordance with the Program Manager's request, no detailed test report was developed. JITC distributes IO information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive IO status information is available via the JITC System Tracking Program (STP), which is accessible by .mil/.gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) NIPRNet at <http://jit.fhu.disa.mil>. Information related to DISN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at


JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Nexus 7000 series Switch Release NX OS 6.0(1)

<http://www.disa.mil/ucco/>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from U.S. Government civilian or uniformed military personnel at the UCCO; e-mail: disa.meade.ns.list.unified-capabilities-certificaion-office@mail.mil.

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, commercial (520) 538-4347, or e-mail to edward.a.mellon.civ@mail.mil. JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The Tracking Number for the SUT is 1126905.

FOR THE COMMANDER:

3 Enclosures a/s


For RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

DISTRIBUTION (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT),
SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities
Division, J68

Defense Information Systems Agency, GS23

This page intentionally left blank.

ADDITIONAL REFERENCES

- (c) Office of the DoD Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2008, Change 3," September 2011.
- (d) Joint Interoperability Test Command, "ASLAN Component Test Plan (UCTP)," February 2012.
- (e) U.S. Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), "Information Assurance (IA) Assessment of Cisco Nexus 7000 (Tracking Number 1126905)," 8 June 2012.

This page intentionally left blank.

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Nexus 7000 series Switch with Release NX OS 6.0(1)

2. SPONSOR. Program Manager (PM) Installation Information Infrastructure Modernization Program (I3MP), point of contact (POC): Mr. Jordan Silk, United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), Building 53302, Fort Huachuca, Arizona 85613; e-mail: jordan.r.silk.civ@mail.mil.

3. SYSTEM POC. Mr. Josh Ament, 7025-2 Kit Creek Rd., Research Triangle Park, North Carolina 27709, e-mail: certteam@cisco.com, website: www.cisco.com/go/govcerts.

4. TESTER. USAISEC TIC, Fort Huachuca, Arizona.

5. SYSTEM DESCRIPTION. The Cisco Nexus 7000 series Switch with Release NX OS 6.0(1) is hereinafter referred to as System Under Test (SUT). The SUT is used to transport voice signaling and media as part of an overall Voice over Internet Protocol (VoIP) system. The SUT provides availability, security, and Quality of Service (QoS) to meet the operational requirements of the network and Assured Services for the Warfighter. However, there are restrictions on the SUT functioning as a Core or Distribution switch. These restrictions are discussed in the following tables within this Certification Testing Summary. The SUT is certified as a Core, Distribution, and Layer 2/Layer 3 Access switch and is interoperable for joint use with other Assured Services Local Area Network (ASLAN) components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10/100/1000BaseT and 1000BaseX for access; and 1000BaseT and 1000/10000BaseX for uplink. All of these interfaces were tested with the exception of the 10BaseT interface. Joint Interoperability Test Command (JITC) analysis determined that the 10BaseT interface is a low risk for certification based on the vendor's Letter of Compliance (LoC) to comply with the Institute of Electrical and Electronics Engineers (IEEE) 802.3i standard and the testing data collected at all other data rates. The Cisco N7K-C7010 switch was tested; however, the Cisco N7K-C7018 and N7K-C7009 employ the same software and similar hardware as the SUT. JITC analysis determined these systems to be functionally identical for IO certification purposes.

6. OPERATIONAL ARCHITECTURE. Figure 2-1 depicts an ASLAN notional operational architecture that in which the SUT may be used. The SUT is certified to support Assured Services within an ASLAN. If a component meets the minimum requirements for deployment in an ASLAN, it also meets the lesser requirements for deployment in a non-ASLAN. Non-ASLANs are "commercial grade" and provide support to Command and Control (C2) (ROUTINE calls only) (C2(R)) or non-C2 voice subscribers. When deployed in a non-ASLAN, the SUT may also be used to receive all levels of precedence, but is limited to supporting calls that are originated at ROUTINE

precedence only. Non-ASLANs do not meet the availability or redundancy requirements for C2 or Special C2 users, and therefore, are not authorized to support precedence calls originated above ROUTINE.

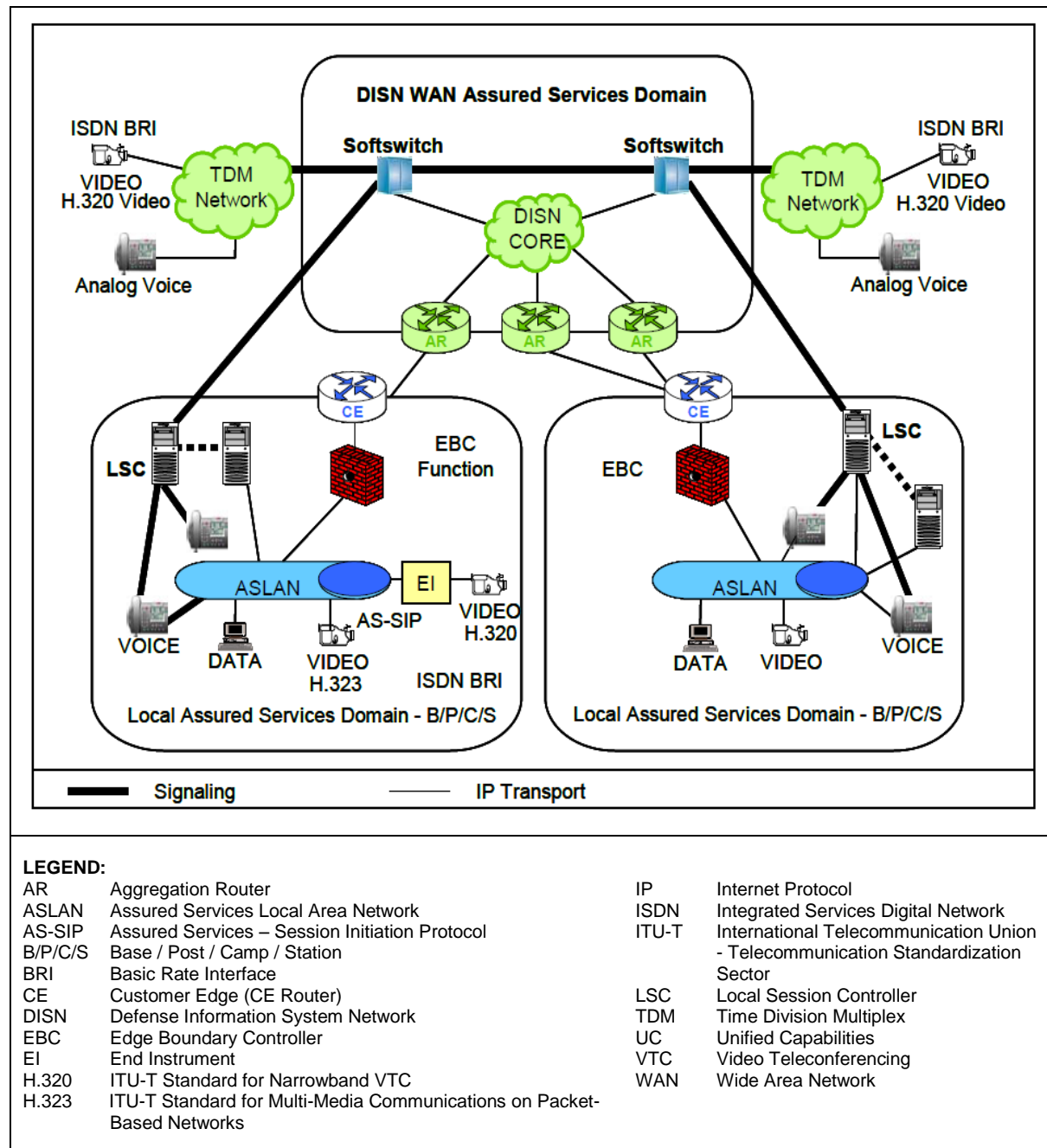


Figure 2-1. DISN UC Notional Operational Architecture

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CR) and Functional Requirements (FR), Information Assurance (IA), and other requirements for ASLAN infrastructure products are established by Section 5.3.1 of Reference (c).

7.1 Interfaces. Table 2-1 depicts the physical ASLAN Product interfaces and the associated standards.

Table 2-1. ASLAN Products Interface Requirements

Interface	UCR 2008, Change 3 Reference	Criteria ¹	Applicability		
			Co	D	A
Serial	5.3.1.3.9	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for applicable EIA/TIA standard.	C	C	C
10Base-X ²	5.3.1.3.1	Support minimum threshold CRs/FRs 1-6 and meet interface criteria for IEEE 802.3i or 802.3j.	C	C	C
100Base-X ²	5.3.1.3.1	Support minimum threshold CRs/FRs 1-6 and meet interface criteria for IEEE 802.3u.	R	R	C
1000Base-X ²	5.3.1.3.1	Support minimum threshold CRs/FRs 1-6 and meet interface criteria for IEEE 802.3z, or 802.3ab.	R	R	C
10000Base-X ²	5.3.1.3.1	Support minimum threshold CRs/FRs 1-6 and meet interface criteria for IEEE 802.3ae.	C	C	C
802.11a	5.3.1.3.1 and 5.3.1.7.2	1-6	C	C	C
802.11b	5.3.1.3.1 and 5.3.1.7.2	1-6	C	C	C
802.11g	5.3.1.3.1 and 5.3.1.7.2	1-6	C	C	C
802.11n	5.3.1.3.1 and 5.3.1.7.2	1-6	C	C	C
802.16	5.3.1.3.1 and 5.3.1.7.2	1-6	C	C	C
NOTES: 1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 2-2. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3. 2. Core and Distribution products must minimally support 100Base-X (802.3u) and 1000Base-X (802.3z). Access products must minimally support one of the following standards: 802.3i (10BaseT), 802.3j (10BaseF), 802.3u (100BaseTX/FX), 802.3z (1000Base-X), or 802.3ab (1000BaseT). Other rates and standards may be provided as conditional interfaces.					

Table 2-1. ASLAN Products Interface Requirements (continued)

LEGEND:			
802.3ab	1000BaseT Gbps Ethernet Over Twisted Pair at 1 Gbps (125 Mbps)	A	Access
802.3ae	10 Gbps Ethernet	ASLAN	Assured Services Local Area Network
802.3i	10BaseT Mbps Over Twisted Pair	C	Conditional
802.3j	10 Mbps Over Fiber	Co	Core
802.3u	Standard for Carrier Sense Multiple Access with Collision Detection at 100 Mbps	CR	Capability Requirement
802.3z	Gigabit Ethernet Standard	D	Distribution
802.11/16	IEEE Wireless Standards	EIA/TIA	Electronics Industries Alliance/ Telecommunications Industry Association
10BaseF	10 Mbps Ethernet Over Fiber	FR	Functional Requirement
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	Gbps	Gigabits Per Second
10Base-X	10 Mbps Ethernet Over Fiber or Copper	ID	Identification
100BaseFX	100 Mbps Ethernet Over Fiber	IEEE	Institute of Electrical and Electronic Engineers
100BaseTX	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	Mbps	Megabits Per Second
100Base-X	100 Mbps Ethernet Over Fiber or Copper	R	Required
1000BaseFX	1000 Mbps Ethernet over fiber	SUT	System Under Test
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	UCR	Unified Capabilities Requirements
1000Base-X	1000 Mbps Ethernet Over Fiber or Copper		
10000Base-X	10000 Mbps Ethernet Over Fiber or Copper		

7.2 CR and FR. Switches have required and conditional features and capabilities that are established by Section 5.3.1 of the Unified Capabilities Requirements (UCR) 2008, Change 3, Reference (c). The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements. The SUTs' features and capabilities and its aggregated requirements in accordance with (IAW) the ASLAN requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of Enclosure 3.

Table 2-2. ASLAN CRs and FRs

CR/FR ID	Capability/Function	Applicability ¹	UCR 2008, Change 3 Reference	Remarks
1	General Performance Parameters			
	Performance Parameters	Required	5.3.1.3	
	Port Interface Rates	Required	5.3.1.3.1	
	Port Parameter Requirements	Required	5.3.1.3.2	
	Class of Service Markings	Required	5.3.1.3.3	
	VLAN Capabilities	Required	5.3.1.3.4	
	Protocols	Required	5.3.1.3.5	
	QoS Features	Required	5.3.1.3.6	
	Network Monitoring	Required	5.3.1.3.7	
	Security	Required	5.3.1.3.8 ²	
2	E2E Performance Requirements			
	Voice Services	Required	5.3.1.4.1	
	Video Services	Required	5.3.1.4.2	
	Data Services	Required	5.3.1.4.3	

Table 2-2. ASLAN CRs and FRs (continued)

3	NM Requirements			
	Configuration Control	Required	5.3.1.6.1	
	Operational Changes	Required	5.3.1.6.2	
	Performance Monitoring	Required	5.3.1.6.3	
	Alarms	Required	5.3.1.6.4	
	Reporting	Required	5.3.1.6.5	
4	Engineering Requirements			
	Physical Media	Required	5.3.1.7.1	Site requirement
	Wireless	Conditional	5.3.1.7.2	
	Traffic Engineering	Required	5.3.1.7.3	Site requirement
	Availability	Required	5.3.1.7.6	Partially driven by topology
	Redundancy	Required	5.3.1.7.7	
5	MPLS			
	MPLS Requirements	Conditional	5.3.1.8.4.1	
	MPLS VPN Augmentation to VLANs	Conditional	5.3.1.8.4.2	
6	IPv6 Requirements			
	Product Requirements	Required	5.3.5.4	

NOTES:

1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. The SUT does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements.

2. Refers to IA requirements for UCR 2008, Change 3, Section 5.4. Detailed IA requirements are included in Reference (e).

LEGEND:

ASLAN

Assured Services Local Area Network

CR

Capability Requirement

E2E

End-to-End

FR

Functional Requirement

IA

Information Assurance

ID

Identification

IPv6

Internet Protocol Version 6

MPLS

Multiprotocol Label Switching

NM

Network Management

QoS

Quality of Service

SUT

System Under Test

UCR

Unified Capabilities Requirements

VLAN

Virtual Local Area Network

VPN

Virtual Private Network

7.3 Information Assurance. Table 2-3 details the IA requirements applicable to the ASLAN products.

Table 2-3. ASLAN Products IA Requirements

Requirement	Applicability (See note.)	UCR 2008, Change 3 Reference	Criteria
General Requirements	Required	5.4.6.2	Detailed requirements and associated criteria for ASLAN products are listed in Reference (c) Section 5.4.
Authentication	Required	5.4.6.2.1	
Integrity	Required	5.4.6.2.2	
Confidentiality	Required	5.4.6.2.3	
Non-Repudiation	Required	5.4.6.2.4	
Availability	Required	5.4.6.2.5	
NOTE: The annotation of ‘required’ refers to a high-level requirement category. Refers to IA requirements for UCR 2008, Change 3, Section 5.4.			
LEGEND:			
ASLAN	Assured Services Local Area Network		
IA	Information Assurance		
	UCR	Unified Capabilities Requirements	

7.4 Other. None

8. TEST NETWORK DESCRIPTION. The SUT was tested at the USAISEC TIC, a Department of Defense (DoD) component test lab, in a manner and configuration similar to that of a notional operational environment. The UCR 2008, Change 3, operational Defense Information System Network (DISN) Architecture is depicted in Figure 2-2, which depicts the relationship of the ASLAN and non-ASLAN to the DISN switch types. Testing the system's required functions and features was conducted using the test configurations depicted in Figure 2-3. Figure 2-3 depicts the ASLAN components in a heterogeneous configuration with Brocade and Enterasys ASLAN components. The SUT was not tested in a homogenous network.

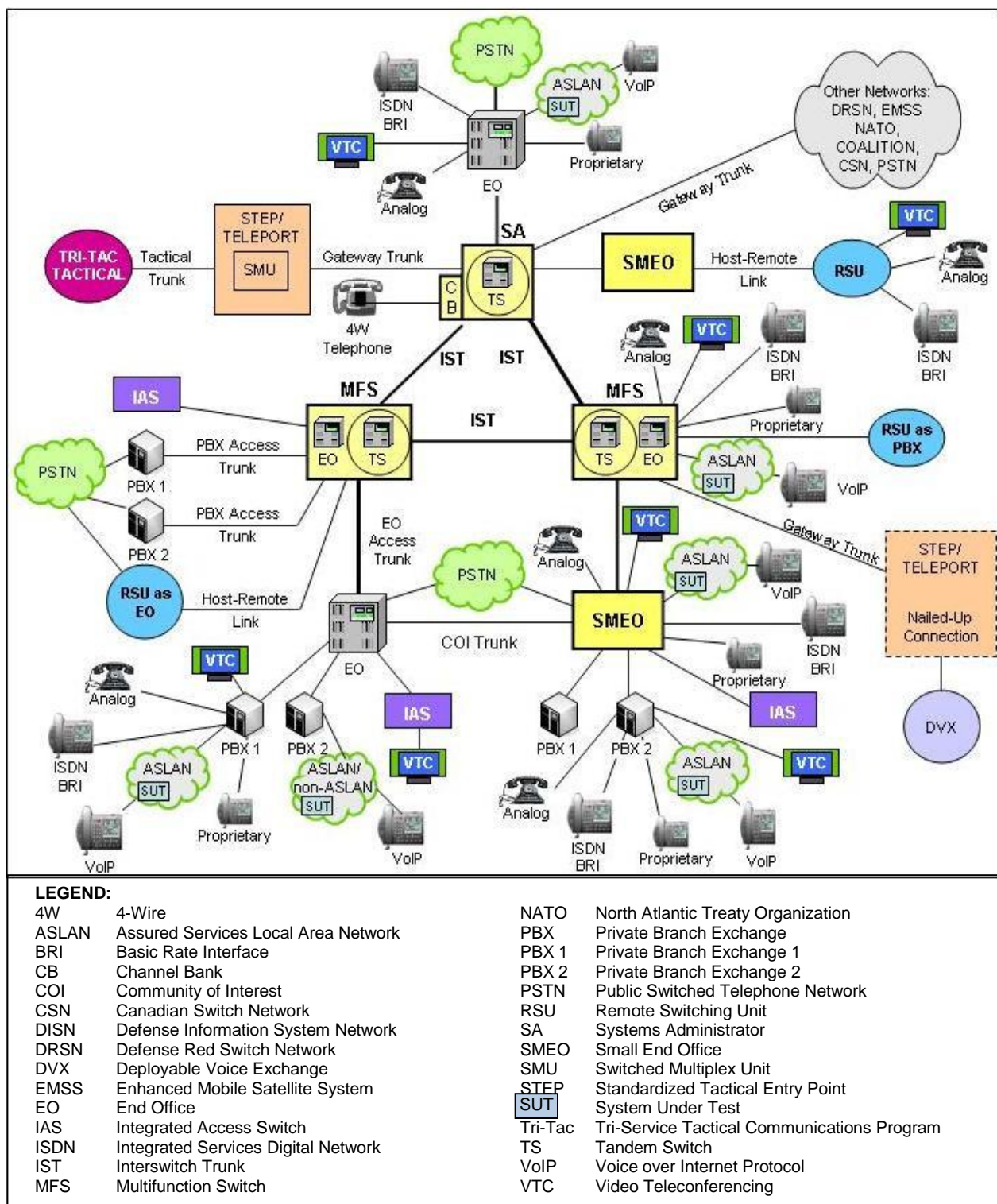


Figure 2-2. DISN Architecture

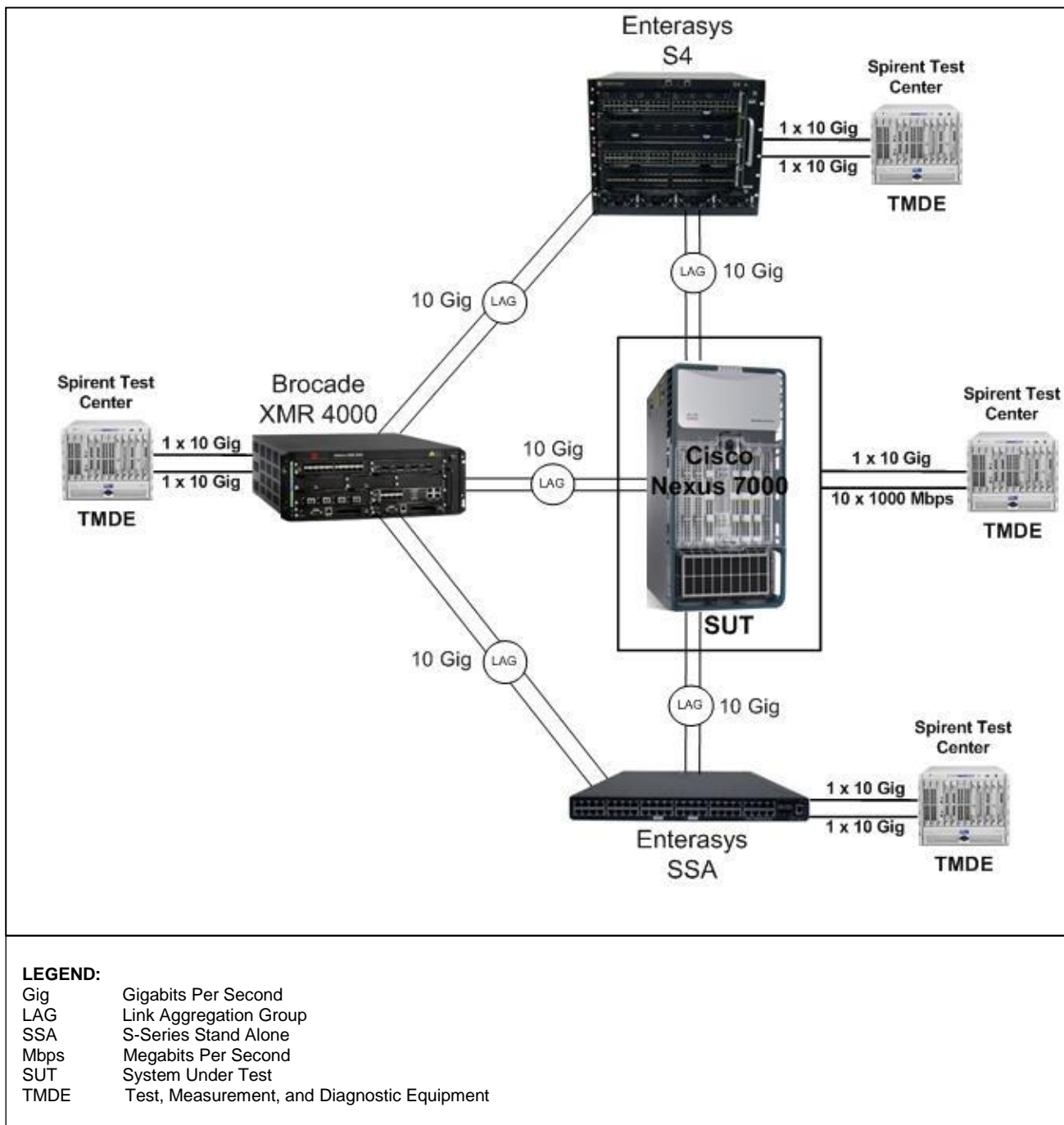


Figure 2-3. Heterogeneous Test Configuration with Brocade and Enterasys

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configuration, hardware, and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its IO capability with associated network devices and network traffic.

Table 2-4. Tested System Configurations

System Name			Release	
Brocade NetIron XMR 4000			5.1	
Enterasys S4			7.41	
Enterasys SSA			7.41	
SUT ¹	Release	Function	Sub-component ¹	Description
Cisco <u>N7K-C7010</u> , N7K-C7018, N7K-C7009	NX OS 6.0(1)	Core, Distribution, Access	<u>N7K-SUP1</u>	<u>Cisco Nexus 7000 Series Supervisor Module</u>
			<u>N7K-C7010-FAB-2</u>	<u>Cisco Nexus 7000 - 10 Slot Chassis - 110Gbps/Slot Fabric Module</u>
			N7K-C7009-FAB-2	Cisco Nexus 7000 9-Slot Chassis 110Gbps/Slot Fabric Module
			N7K-C7018-FAB-2	Cisco Nexus 7000 - 18 Slot Chassis - 110Gbps/Slot Fabric Module
			<u>N7K-M148GT-11</u>	<u>Cisco Nexus 7000 Series 48-Port 10/100/1000 Mbps Ethernet Copper Module</u>
			<u>N7K-M148GS-11</u>	<u>Cisco Nexus 7000 Series 48-Port GigE Fiber Module (SFP)</u>
			<u>N7K-M148GS-11L</u>	<u>Cisco Nexus 7000 Series 48-Port GigE Fiber Module with XL Option (SFP)</u>
			N7K-M148GT-11L	Cisco Nexus 7000 Series 48-Port 10/100/1000 Mbps Ethernet Copper Module with XL Option (RJ45)
			<u>N7K-M108X2-12L</u>	<u>Cisco Nexus 7000 Series 8-Port 10GigE Fiber Module (X2 optics)</u>
			<u>N7K-M132XP-12L</u> ^{2,3}	Cisco Nexus 7000 Series 32-Port 10GigE Fiber Module with XL Option
			<u>N7K-F132XP-15</u>	<u>Cisco Nexus 7000 - 32-Port 1GigE/10GigE Fiber Module, SFP/SFP+ (Layer 2 only)</u>
			<u>N7K-F248XP-25</u>	<u>Cisco Nexus 7000 F2-Series 48-Port 1GigE/10GigE Fiber Module (SFP/SFP+)</u>

Table 2-4. Tested System Configurations (continued)

SUT ¹	Release	Function	Sub-component ¹	Description
Cisco <u>N7K-C7010</u> , N7K-C7018, N7K-C7009	NX OS 6.0(1)	Core, Distribution, Access	The following modules were certified during previous ASLAN certifications and recertified based on technology maturity per UCR 2008, Change 3, Section 4.4.2:	
			N7K-M132XP-12 ^{2,3}	Cisco Nexus 7000 Series 32-Port 10GigE Fiber Module with 80Gbps Fabric (SFP+)
			N7K-C7010-FAB-1	Cisco Nexus 7000 10-Slot Chassis 46Gbps/Slot Fabric Module
			N7K-C7018-FAB-1	Cisco Nexus 7000 18-Slot Chassis 46Gbps/Slot Fabric Module
NOTE: 1. Components bolded and underlined were tested by the USAISEC TIC. The other components in the family series were not tested; however, they utilize the same OS software and similar hardware as the SUT. JITC analysis determined them to be functionally identical for IO certification purposes. As such, they are also certified for joint use. 2. The SUT complies with the Non-blocking requirement in the Performance Parameters IAW UCR 2008, Change 3, Section 5.3.1.3, Paragraph 1 as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the “Performance Mode” (see deployment guide) with the following modules: N7K-M132XP-12L and N7K-M132XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the “Default Mode” or “Oversubscription Mode” would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the “Default” or “Oversubscription” mode of operation. 3. The SUT complies with the QoS blocking factor features IAW UCR 2008, Change 3, Section 5.3.1.3.6, Paragraph 5b as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the “Performance Mode” (see deployment guide) with the following modules: N7K-M132-XP-12L and N7K-M132-XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the “Default Mode” or “Oversubscription Mode” would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the “Default” or “Oversubscription” mode of operation.				
LEGEND: ASLAN Assured Services Local Area Network DISA Defense Information Systems Agency GigE Gigabit Ethernet Gbps Gigabits Per Second IO Interoperability JITC Joint Interoperability Test Command Mbps Megabits Per Second Nx Nexus OS Operating System QoS Quality of Service SFP+ Small Form-Factor Pluggable Plus SUT System Under Test TIC Technology Integration Center UCR Unified Capabilities Requirements USAISEC U.S. Army Information Systems Engineering Command				

10. TESTING LIMITATIONS. None.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical IO requirements for a Core, Distribution, and Layer 2/Layer 3 Access switch IAW UCR 2008, Change 3, Section 5.3.1, and is certified for joint use with other network infrastructure products listed on the UC APL. Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-5.

Table 2-5. SUT Interface Requirements Status

Interface	Applicability			UCR 2008, Change 3 Reference	Threshold CR/FR ¹	Status	Remarks
	Co	D	A				
Serial	C	C	C	5.3.1.3.9	1-4	Certified	The SUT met the CRs and FRs with the following standard: EIA-232.
10Base-X	C	C	C ²	5.3.1.3.1	1-6	Certified ³	The SUT met CRs and FRs with the following IEEE standard: 802.3i (10BaseT).
100Base-X	R	R	C ²	5.3.1.3.1	1-6	Certified	The SUT met CRs and FRs with the following IEEE standard: 802.3u (100BaseT).
1000Base-X	R	R	C ²	5.3.1.3.1	1-6	Certified	The SUT met CR and FRs with the following IEEE standards: 802.3ab (1000BaseT), 802.3z (1000Base-SX, 1000Base-LX).
10000Base-X	C	C	C	5.3.1.3.1	1-6	Certified	The SUT met CRs and FRs with the following IEEE standard: 802.3ae (10GBase-SR, 10GBase-LR).
802.11a	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.11b	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.11g	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.11n	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
802.16	C	C	C	5.3.1.3.1/5.3.1.7.2	1-6	Not Supported ⁴	N/A
NOTES: 1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3. 2. Core and Distribution products must minimally support 100Base-X (802.3u) and 1000Base-X (802.3z). Access products must minimally support one of the following standards: 802.3i (10BaseT), 802.3j (10BaseF), 802.3u (100BaseT/F), 802.3z (1000BaseF), or 802.3ab (1000BaseT). Other rates and standards may be provided as conditional interfaces. 3. The USAISEC TIC tested all these interfaces with the exception of the 10BaseT interface. JITC analysis determined that the 10BaseT interface is a low risk for certification based on the vendor's LoC to the IEEE 802.3i and the testing data collected at all other data rates. 4. The SUT does not support this interface. This interface is not required for a Core, Distribution, or Access switch.							

Table 2-5. SUT Interface Requirements Status (continued)

LEGEND:		A	Access
802.3ab	1000BaseT Gbps Ethernet Over Twisted Pair at 1 Gbps (125 Mbps)	C	Conditional
802.3ae	10 Gbps Ethernet	Co	Core
802.3i	10BaseT Mbps Over Twisted Pair	CR	Capability Requirement
802.3j	10 Mbps Over Fiber	D	Distribution
802.3u	Standard for Carrier Sense Multiple Access with Collision Detection at 100 Mbps	EIA	Electronic Industries Alliance
802.3z	Gigabit Ethernet Standard	EIA-232	Standard for Defining the Mechanical and Electrical Characteristics for Connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) Data Communications Devices
802.11/16	IEEE Wireless Standards	FR	Functional Requirement
10BaseF	10 Mbps Ethernet Over Fiber	Gbps	Gigabits Per Second
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	ID	Identification
10Base-X	10 Mbps Ethernet Over Fiber or Copper	IEEE	Institute of Electrical and Electronics Engineers
100BaseF	100 Mbps Ethernet Over Fiber	JITC	Joint Interoperability Test Command
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	LoC	Letter of Compliance
100Base-X	100 Mbps Ethernet Over Fiber or Copper	LR	Long Range Optics
1000BaseF	1000 Mbps Ethernet Over Fiber	LX	Single-Mode Fiber Optics
1000Base-LX	1000 Mbps Ethernet Over Fiber	Mbps	Megabits Per Second
1000Base-SX	1000 Mbps Ethernet Over Fiber	N/A	Not Applicable
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	R	Required
1000Base-X	1000 Mbps Ethernet Over Fiber or Copper	SR	Short Range Optics
10000Base-X	10000 Mbps Ethernet Over Fiber or Copper	SX	Multi-Mode Fiber Optics
10GBase-LR	10000 Mbps Ethernet Over Fiber	SUT	System Under Test
10GBase-SR	10000 Mbps Ethernet Over Fiber	TIC	Technology Integration Center
		UCR	Unified Capabilities Requirements
		USAISEC	U.S. Army Information Systems Engineering Command

11.2 CR and FR. The SUT CR and FR status is depicted in Table 2-6. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

Table 2-6. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability ¹	UCR 2008, Change 3 Reference	Status	Remarks
1	General Performance Parameters				
	Performance Parameters	Required	5.3.1.3	Partially Met ²	
	Port Interface Rates	Required	5.3.1.3.1	Met	
	Port Parameter Requirements	Required	5.3.1.3.2	Partially Met ³	
	Class of Service Markings	Required	5.3.1.3.3	Met	
	VLAN Capabilities	Required	5.3.1.3.4	Met	
	Protocols	Required	5.3.1.3.5	Partially Met ⁴	
	QoS Features	Required	5.3.1.3.6	Partially Met ⁵	
	Network Monitoring	Required	5.3.1.3.7	Met	
	Security	Required	5.3.1.3.8	Met	
2	E2E Performance Requirements				
	Voice Services	Required	5.3.1.4.1	Met ⁶	
	Video Services	Required	5.3.1.4.2	Met ⁶	
	Data Services	Required	5.3.1.4.3	Met ⁶	
3	NM Requirements				
	Configuration Control	Required	5.3.1.6.1	Met	
	Operational Changes	Required	5.3.1.6.2	Met	
	Performance Monitoring	Required	5.3.1.6.3	Met	
	Alarms	Required	5.3.1.6.4	Met	
	Reporting	Required	5.3.1.6.5	Met	
4	Engineering Requirements				
	Physical Media	Required	5.3.1.7.1	Met ⁷	
	Wireless	Conditional	5.3.1.7.2	Not Tested ⁸	
	Traffic Engineering	Required	5.3.1.7.3	Met ⁷	
	Availability	Required	5.3.1.7.6	Met ⁷	
	Redundancy	Required	5.3.1.7.7	Met ⁷	
5	MPLS				
	MPLS Requirements	Conditional	5.3.1.8.4.1	Not Tested ⁸	
	MPLS VPN Augmentation to VLANs	Conditional	5.3.1.8.4.2	Not Tested ⁸	
6	IPv6 Requirements				
	Product Requirements	Required	5.3.5.4	Partially Met ⁴	

Table 2-6. SUT CRs and FRs Status (continued)

NOTES:

1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. The SUT does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements.
2. The SUT complies with the Non-blocking requirement in the Performance Parameters IAW UCR 2008, Change 3, Section 5.3.1.3, Paragraph 1 as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the "Performance Mode" (see deployment guide) with the following modules: N7K-M132XP-12L and N7K-M132XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the "Default Mode" or "Oversubscription Mode" would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the "Default" or "Oversubscription" mode of operation.
- 3 The SUT does not support the following Port Parameter Requirements: Link Layer Discovery – Media Endpoint Discovery IAW ANSI/TIA-1057, and Power over Ethernet IAW 802.3af or 802.3at-2009. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as minor. The Power over Ethernet is not supported because the SUT is designed as a Data Center switch. In addition, DISA determined this requirement will change to "optional" in future UCR documents (e.g. UCR 2013).
4. The SUT does not support the following Protocols RFCs: 2560, 3273, 4552, and 5798. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as minor. DoD sites deploying OSPFv3 should use ACLs to secure OSPF until RFC 4552 is supported.
5. The SUT complies with the QoS blocking factor features IAW UCR 2008, Change 3, Section 5.3.1.3.6, Paragraph 5b as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the "Performance Mode" (see deployment guide) with the following modules: N7K-M132-XP-12L and N7K-M132-XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the "Default Mode" or "Oversubscription Mode" would have a critical impact on operations and therefore the SUT is not certified for use on the DISN as a Core or Distribution switch with the above modules in either the "Default" or "Oversubscription" mode of operation.
6. This requirement was verified and met using simulated voice, video, and data traffic in an operational emulated environment to meet E2E requirements. The SUT must be deployed IAW deployment guide and engineering guidelines in UCR 2008, Change 3, Section 5.3.1.4.
7. This requirement was met with the following stipulations: It is the site's responsibility to configure the SUT in a manner which meets the engineering requirements listed in Section 11.2 d. of Enclosure 2, and that it does not create a single point of failure which could impact more than 96 C2 users.
8. Wireless and MPLS were not tested and are not certified for joint use. Wireless and MPLS are conditional and, therefore, not required for a Core, Distribution, or Access switch.

LEGEND:

802.3af	Power Over Ethernet	IPv6	Internet Protocol Version 6
802.3at-2009	Power Over Ethernet Plus	MPLS	Multiprotocol Label Switching
ACL	Access Control List	NM	Network Management
ANSI	American National Standards Institute	OSPF	Open Shortest Path First
C2	Command and Control	OSPFv3	Open Shortest Path First Version 3
CR	Capability Requirement	POA&M	Plan of Action and Milestones
DISA	Defense Information Systems Agency	QoS	Quality of Service
DoD	Department of Defense	RFC	Request For Comment
E2E	End-to-End	SUT	System Under Test
FR	Functional Requirement	TIA	Telecommunications Industry Association
IAW	In Accordance With	UCR	Unified Capabilities Requirements
ID	Identification	VLAN	Virtual Local Area Network
IPv4	Internet Protocol Version 4	VPN	Virtual Private Network

a. General Performance Parameters: Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6).

(1) Performance Parameters IAW UCR 2008, Change 3, Section 5.3.1.3. The SUT met the performance parameters depicted in the UCR 2008, Change 3, Section 5.3.1.3, with both testing and vendor's LoC. The SUT operated in the required 50-percent non-blocking mode on all interfaces for all Core and Distribution layers with the

following exceptions: The SUT complies with the Non-blocking requirement in the Performance Parameters IAW UCR 2008, Change 3, Section 5.3.1.3, Paragraph 1 as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the “Performance Mode” with the following modules: N7K-M132XP-12L and N7K-M132XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the “Default Mode” or “Oversubscription Mode” would have a critical impact on operations and is not a certified configuration.

(2) Port Interface Rates. The UCR 2008, Change 3, Section 5.3.1.3.1, states that Core and Distribution products shall minimally support 100 Megabits per second (Mbps) IAW IEEE 802.3u and 1 Gigabit per second (Gbps) IAW with IEEE 802.3z. Access products must minimally provide one of the following interface rates: 10 Mbps IAW IEEE 802.3i and j, 100 Mbps IAW IEEE 802.3u, and 1000 Mbps IAW IEEE 802.3z and 802.3ab. The SUT is certified as interoperable for joint use with other ASLAN components listed on the UC APL with the following interfaces: 10/100/1000BaseT and 100/1000BaseX for access, and 1000BaseT and 1000/10GBaseX for uplink. All of these interfaces were tested with the exception of the 10BaseT interface. JITC analysis determined that the 10BaseT interface is a low risk for certification based on the vendor’s LoC to comply with the IEEE 802.3i standard and the testing data collected at all other data rates. All the SUT interfaces linked up at the required rates and negotiated for the correct rates, which met this requirement.

(3) Port Parameter Requirements. The UCR 2008, Change 3, section 5.3.1.3.2, states that Core, Distribution, and Access products shall provide the following parameters on a per port basis: Auto-negotiation IAW IEEE 802.3, Force mode IAW IEEE 802.3, and Filtering IAW Request for Comments RFC 1812. Port parameters were configurable and conformed to the requirements. The vendor met these requirements with testing and the vendor’s LoC, with the exception of the vendor’s LoC Link Layer Discovery – Media Endpoint Discovery IAW ANSI/TIA-1057, and Power over Ethernet (PoE) IAW 802.3af or 802.3at-2009. On 10 July 2012, DISA has accepted and approved the vendor’s POA&M and adjudicated this discrepancy as minor. The Power over Ethernet is not supported because the SUT is a Data Center switch, so it is not design to support PoE. In addition, the PoE applicability will change to “optional” in future UCR documents (e.g. UCR 2013).

(4) Class of Service (CoS) Markings. The UCR 2008, Change 3, Section 5.3.1.3.3, states that the SUT shall support Differentiated Services Code Points (DSCPs) for both IPv4 and IPv6, as shown in the sub-paragraphs below. The SUT met these requirements with both testing and the vendor’s LoC.

(a) Accept any packet tagged with a DSCP value (0-63) on an ingress port and assign that packet to a QoS behavior.

(b) Accept any packet tagged with a DSCP value (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63).

(c) Support the prioritization of aggregate service classes with queuing according to QoS features.

(5) Virtual Local Area Network (VLAN) Capabilities. The SUT met VLAN capabilities IAW UCR 2008, Change 3, Section 5.3.1.3.4, with testing and the vendor's LoC. The VLAN markings were preserved on the SUT, VLAN tagged traffic was separated and managed according to IEEE 802.1q. The SUT successfully performed both port-based and address-based VLANs and can assign any VLAN tag any value from 1 through 4094 (0 and 4095 are excluded), which met this requirement.

(6) Protocols. The SUT met all of the protocols IAW UCR 2008, Change 3, Section 5.3.1.3.5, for IPv4 and Section 5.3.5 for IPv6 by testing and the vendor's LoCs with the following exceptions: The SUT did not meet RFCs 2560, 3273, 4552, and 5798. On 10 July 2012, DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as minor.

(7) QoS Features. The UCR 2008, Change 3, Section 5.3.1.3.6, states that the Core, Distribution, and Access products shall be capable of providing a minimum of four queues, assign any "tagged" session to any of the queues, support Differentiated Services per hop behaviors and traffic conditioning with an assigned bandwidth percentage per queue, and meet traffic conditioning requirements. The SUT QoS, which includes rate-shaping, performed as configured. All variance was within the limitation of resolution of the test instruments. The test equipment recorded that the higher prioritized traffic was properly queued above lower prioritized best effort traffic; therefore, the SUT met this requirement with the following exceptions: The SUT complies with the QoS blocking factor as an Access switch in all modes of operation for all modules listed in Table 1. However, the SUT only complies with this requirement for Core and Distribution in the "Performance Mode" with the following modules: N7K-M132-XP-12L and N7K-M132-XP-12. DISA adjudicated this limitation on use of these modules with the SUT as minor. Configuring the SUT as a Core or Distribution layer switch with these modules in the "Default Mode" or "Oversubscription Mode" would have a critical impact on operations and is not a certified configuration.

(8) Network Monitoring. The UCR 2008, Change 3, Section 5.3.1.3.7, states that Core, Distribution, and Access products shall support network monitoring features. Network Monitoring via Simple Network Management Protocol (SNMP) was evaluated by the USAISEC TIC-led IA test teams and published in a separate report, Reference (e). Based on this evaluation, the SUT met all requirements.

(a) SNMP IAW RFCs 3411, 3412, 3413, 3414, 3415, 3416, and 3417. The SUT met the requirements through the vendor's LoC and testing. The SilverCreek SNMP Test Suite was used to capture SNMP traps. For the port configuration change

test, the speed of an individual port on each switch was changed from 1000 Mbps to 100 Mbps and back again.

(b) Remote Monitoring (RMON) IAW RFC 2819. The SUT met this requirement through the vendor's LoC.

(c) Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584. The SUT met this requirement through the vendor's LoC.

(d) Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. Security was tested by USAISEC TIC-led IA test teams, and the results were published in a separate report, Reference (e).

(9) Security. The UCR 2008, Change 3, Section 5.3.1.3.8, states that the Core, Distribution, and Access products shall meet the security protocol requirements listed in UCR 2008, Change 3, Section 5.4. Security testing was accomplished via USAISEC TIC-led IA test teams and published in a separate report, Reference (e).

b. End-to-End (E2E) Performance Requirements. These requirements were verified using simulated voice, video, and data traffic in an emulated operational environment. To meet E2E requirements the SUT must be deployed IAW deployment and engineering guidelines provided in UCR 2008, Change 3, Section 5.3.1.4. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering). The E2E performance was evaluated in a heterogeneous configuration, as depicted in Figure 2-3.

(1) Voice Services

a. Latency. The UCR 2008, Change 3, Section 5.3.1.4.1.1, states that latency shall not be more than 6 ms E2E across the ASLAN over any 5-minute measured period under congested conditions. The measured latency for the SUT was 0.068 ms, which met the requirement.

b. Jitter. The UCR 2008, Change 3, Section 5.3.1.4.1.2, states that when transporting voice Internet Protocol (IP) packets, the E2E jitter shall not exceed 3 ms over any 5-minute measured period under congested conditions. The measured jitter for the SUT was 0.002 ms, which met the requirement.

c. Packet Loss. The UCR 2008, Change 3, Section 5.3.1.4.1.3, states that actual measured packet loss across the local area network (LAN) shall not exceed 0.045 percent within the defined queuing parameters. The packet loss requirement shall be achievable over any five-minute measured period under congested conditions. The measured packet loss for the SUT was 0.00 percent, which met the requirement.

(2) Video Services

a. Latency. The UCR 2008, Change 3, Section 5.3.1.4.2.1, states that latency shall not exceed 30 ms E2E across the ASLAN over any 5-minute period measured under congested conditions. The measured latency for the SUT was 0.109 ms, which met the requirement.

b. Jitter. The UCR 2008, Change 3, Section 5.3.1.4.2.2, states that when transporting voice IP packets E2E jitter shall not exceed 30 ms over any 5-minute measured period under congested conditions. The measured jitter for the SUT was 0.002 ms, which met the requirement.

c. Packet Loss. The UCR 2008, Change 3, Section 5.3.1.4.2.3, states that actual measured packet loss across the LAN shall not exceed 0.15 percent within the defined queuing parameters. The packet loss requirement shall be achievable over any 5-minute measured period under congested conditions. The measured packet loss for the SUT was 0.00 percent, which met the requirement.

(3) Data Services

a. Latency. The UCR 2008, Change 3, Section 5.3.1.4.3.1, states that latency for prioritized data IP packets shall not exceed 45 ms E2E across the ASLAN over any 5-minute period as measured under congested conditions. The measured latency for the SUT was 0.101 ms for Preferred Data and 0.132 ms for Best Effort Data, which met the requirement.

b. Jitter. The UCR 2008, Change 3, Section 5.3.1.4.3.2 states that there are no jitter requirements for preferred data IP packets.

c. Packet Loss. The UCR 2008, Change 3, Section 5.3.1.4.3.3, states that actual measured packet loss across the LAN shall not exceed 0.15 percent within the defined queuing parameters. The packet loss requirement shall be achievable over any 5-minute measured period under congested conditions. The measured packet loss for the SUT was 0.00 percent for both Preferred Data and Best Effort Data, which met the requirement.

c. Network Management (NM) Requirements. The NM requirements in the subparagraphs below were met by testing and the vendor's LoC and evaluated by USAISEC TIC-led IA test teams, and the results are published in a separate report, Reference (e).

(1) Configuration Control. IAW UCR 2008, Change 3, Section 5.3.1.6.1, the SUT Network Management System (NMS) shall report configuration change events in near-real-time (NRT). The system shall report the success or failure of authorized

configuration change attempts in NRT. NRT is defined as, within five seconds of detecting the event, excluding transport time.

(2) Operational Changes. IAW UCR 2008, Change 3, Section 5.3.1.6.2, LAN infrastructure components must provide metrics to the NMS to allow them to make decisions on managing the network. The SUT NMS shall have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement).

(3) Performance Monitoring. IAW UCR 2008, Change 3, Section 5.3.1.6.3, all LAN components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT. The SUT NMS will have an automated NM capability to obtain the status of networks and associated assets 99 percent of the time (with 99.9 percent as an Objective Requirement) within five seconds of detecting the event, excluding transport. The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss.

(4) Alarms. IAW UCR 2008, Change 3, Section 5.3.1.6.4, all LAN components shall be capable of providing SNMP alarm indications to an NMS. The SUT NMS shall have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving.

(5) Reporting. IAW UCR 2008, Change 3, Section 5.3.1.6.5, to accomplish Global Information Grid E2E situational awareness, an NMS shall have the NM capability of automatically generating and providing an integrated/correlated presentation of network and all associated networks.

d. Engineering Requirements.

(1) Copper Media. IAW UCR 2008, Change 3, Section 5.3.1.7.1, cabling used for the LAN shall not be lower than a Category 5 performance.

(2) Wireless. The UCR 2008, Change 3, Section 5.3.1.7.2, states that wireless LAN implementations are considered as extensions of the physical layer. If an ASLAN supports wireless, it must meet all of the applicable requirements of this section.

(3) Traffic Engineering. IAW UCR 2008, Change 3, Section 5.3.1.7.3, bandwidth in the LAN shall be engineered so Voice IP subscribers do not exceed more than 25 percent of available trunk bandwidth, and no single point of failure within the ASLAN can cause a voice service outage to more than 96 users.

(4) Availability. IAW UCR 2008, Change 3, Section 5.3.1.7.6, system reliability must be engineered for 99.999 percent for FLASH/FLASH OVERRIDE users,

99.997 for IMMEDIATE/PRIORITY users in an ASLAN. ROUTINE users may be supported by a non-ASLAN with a reliability of only 99.9 percent. The C2 users may not be supported by a non-ASLAN. It is the site's responsibility to configure the SUT in a manner which meets the user requirement and does not create a single point of failure, which could impact more than 96 C2 users.

(5) Redundancy. The UCR 2008, Change 3, Sections 5.3.1.2.1, 5.3.1.7.7, 5.3.1.7.7.1, and 5.3.1.7.7.2, state that ASLAN components can have no single point of failure for more than 96 users for C2 and Special C2 users. The UCR 2008, Change 3, Section 5.3.1.7.7, states the following redundancy requirements: redundancy can be met if the product itself provides redundancy internally or a secondary product is added to the ASLAN to provide redundancy to the primary product. Single-product redundancy may be met with a modular chassis that at a minimum provides the following: dual power supplies, dual processors, termination sparing, redundancy protocol, no single point of failure, and switch fabric or backplane redundancy. In the event of a component failure in the network, all active calls shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 5 seconds. If a secondary product has been added to provide redundancy to a primary product, the failover to the secondary product must meet the same requirements. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. The SUT met all of these requirements. All of the redundant components were tested and found to meet all the failover and access requirements with a measured restoral within 5 seconds with no loss of existing active circuits.

e. Multiprotocol Label Switching (MPLS) Requirements. IAW UCR 2008, Change 3, Section 5.3.1.7.8, MPLS may be used to improve the performance of the ASLAN Core layer for implementations covering a large geographical area. MPLS was not evaluated and is not covered under this certification. This is a conditional requirement for a Core, Distribution, or Access switch.

f. IPv6 Requirements. All UC products must meet the IPv6 requirements IAW UCR 2008, Change 3, Section 5.3.5. The IPv6 requirements were met by testing and the vendor's LoC with the exceptions of the following: the SUT does not comply with IPv6 RFCs 4552 and 5798. On 10 July 2012, DISA has accepted and approved the vendor's POA&Ms for the RFC 4552 and 5798 discrepancies and adjudicated this discrepancy as minor. DoD sites deploying OSPFv3 should use ACLs to secure OSPF until RFC 4552 is supported. The SUT was tested and certified for joint use with IPv6 voice, video, and data traffic.

11.3 Information Assurance (IA). Security testing was accomplished via USAISEC TIC-led IA test teams and published in a separate report, Reference (e).

11.4 Other. None

12. TEST AND ANALYSIS REPORT. No detailed test report was developed IAW the Program Manager's request. JITC distributes IO information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive IO status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO); e-mail: disa.meade.ns.list.unified-capabilities-certificaion-office@mail.mil.

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The Assured Services Local Area Networks (ASLAN) components have required and conditional features and capabilities that are established by Section 5.3.1 of the Unified Capabilities Requirements (UCR) 2008, Change 3. The system under test (SUT) does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements. The detailed Functional requirements (FRs) and Capability Requirements (CRs) for ASLAN products are listed in Table 3-1. Detailed Information Assurance (IA) requirements are included in Reference (e).

Table 3-1. ASLAN Products CRs and FRs

ID	Requirement (See note.)		UCR 2008, Change 3 Reference
1	ASLAN components can have no single point of failure for >96 users for C2 and Special C2 users. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. (R)		5.3.1.2.1, 5.3.1.7.7
2	Non-blocking of any voice or video traffic at 50% Core/Distribution (R), 12.5% Non-Blocking Access. (R)		5.3.1.3
3	Maximum of 1 ms of voice jitter for all ASLAN components, 10 ms for video. (R)		5.3.1.3
4	Maximum of 0.015% voice, 0.05% video, and 0.05% Preferred Data packet loss. (R)		5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video. (R)		5.3.1.3
6	100 Mbps IAW IEEE 802.3u and 1 Gbps IAW IEEE 802.3z for Core and Distribution layer components and one of: 10 Mbps IAW IEEE 802.3i/j, 100 Mbps IAW IEEE 802.3u, or 1000 Mbps IAW IEEE 803.3z/ab for Access layer components. (R) May provide Fiber Channel IAW INCITS T11.2/3, but if provided, must support RFC 4338 and RFC 4044. (C)		5.3.1.3.1
7	Force mode and auto-negotiation IAW IEEE 802.3, filtering IAW RFC 1812, and flow control IAW IEEE 802.3x. (R)		5.3.1.3.2
8	Port Parameter Requirements	Auto-negotiation IAW IEEE 802.3. (R)	5.3.1.3.2
9		Force mode IAW IEEE 802.3. (R)	
10		Flow control IAW IEEE 802.3x. (R)	
11		Filtering IAW RFC 1812. (R)	
12		Link Aggregation IAW IEEE 802.1AX (output/egress ports only). (R)	
13		Spanning Tree Protocol IAW IEEE 802.1D. (R)	
14		Multiple Spanning Tree IAW IEEE 802.1s. (R)	
15		Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R)	
16		LLDP IAW IEEE 802.1AB. Core and Distribution (C) Access (R)	
17		Link Layer Discovery- Media Endpoint Discovery IAW ANSI/TIA-1057. Core and Distribution (C) Access (R)	
18		Power over Ethernet IAW either 802.3af-2003 or 802.3at-2009. (R)	
19	Class of Service Marking: L3 DSCPs IAW RFC 2474. (R) L2 3-bit user priority field of the IEEE 802.1Q 2-byte TCI field. (C)		5.3.1.3.3
20	VLAN Capabilities IAW IEEE 802.1Q. (R)		5.3.1.3.4
21	Protocols IAW DISR profile (IPv4 and IPv6). IPv4 (R: LAN Switch, L2 Switch): IPv6 (R: LAN Switch, C: L2 Switch). Note: A L2 switch is required to support only RFCs 2460, 5095, 2464, and be able to queue packets based on DSCPs IAW RFC 2474. Must conform to UCR 2008, Change 3, Table 5.3.1-4.		5.3.1.3.5
22	QoS Features	Shall support minimum of 4 queues. (R)	5.3.1.3.6
23		Must be able to assign VLAN tagged packets to a queue. (R)	
24		Support DSCP PHBs per RFCs 2474, 2597, 3140, and 3246. (R: LAN Switch).	
25		Support RFCs in Table 5.3.1-5, FIFO 3670 (C), and one of the following RFCs: WFQ 3662, CQ 3670, PQ 1046 and CB-WFQ 3366. (R)	
26		Must be able to assign a bandwidth or percent of traffic to any queue. (R)	

Table 3-1. ASLAN Products CRs and FRs (continued)

ID	Requirement (See note.)		UCR 2008, Change 3 Reference
27	Network Monitoring	SNMP IAW RFCs 3411, 3412, 3413, 3414, 3415, 3416 and 3417. (R)	5.3.1.3.7
28		SNMP traps IAW RFC 1215. (R)	
29		Remote monitoring IAW RFC 2819 and AES Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. (R)	
30		Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584. (R)	
31	Product Requirements Summary IAW UCR 2008, Change 3, Table 5.3.1-5. (R)		5.3.1.3.9
32	E2E Performance (Voice)	No more than 6 ms latency over any 5-minute period measured under congestion. (R)	5.3.1.4.1
		No more than 3 ms jitter over any 5-minute period measured under congestion. (R)	
		Packet loss not to exceed 0.045% engineered (queuing) parameters over any 5-minute period under congestion. (R)	
33	E2E Performance (Video)	No more than 30 ms latency over any 5-minute period measured under congestion. (R)	5.3.1.4.2
		No more than 30 ms jitter over any 5-minute period measured under congestion. (R)	
		Packet loss not to exceed engineered 0.15% (queuing) parameters over any 5-minute period under congestion. (R)	
34	E2E Performance (Data)	No more than 45 ms latency over any 5-minute period measured under congestion (R)	5.3.1.4.3
		Packet loss not to exceed 0.15% engineered (queuing) parameters over any 5-minute period under congestion. (R)	
35	LAN Network Management	Configuration Control for ASLAN and non-ASLAN. (R)	5.3.1.6.1
36		Operational Controls for ASLAN and non-ASLAN. (R)	5.3.1.6.2
37		Performance Monitoring for ASLAN and non-ASLAN. (R)	5.3.1.6.3
38		Alarms for ASLAN and non-ASLAN. (R)	5.3.1.6.4
39		Reporting for ASLAN and non-ASLAN. (R)	5.3.1.6.5
40	Redundancy	Redundant Power Supplies. (Required on standalone redundant products.)	5.3.1.7.7
41		Chassis Failover. (Required on standalone redundant products.)	
42		Switch Fabric Failover. (Required on standalone redundant products.)	
43		Non-LACP Link Failover. (R)	
44		Fiber Blade Failover. (R)	
45		Stack Failover. (C) (Required if the stack supports more than 96 users.)	
46		CPU (routing engine) blade Failover. (R)	
47	MPLS	MPLS may not add measurable loss or jitter to system. (C)	5.3.1.8.4.1
48		MPLS conforms to RFCs in UCR 2008, Change 3, Table 5.3.1-14. (C)	5.3.1.8.4.1
49		MPLS Support L2 and L3 VPNs. (C)	5.3.1.8.4.2.1/2
50	IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C)		5.3.5.4
51	IPv6 System Requirements	Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C)	5.3.5.4
52		Support IPv6 packets over Ethernet IAW RFC 2464. (R)	5.3.5.4
53		Support MTU discovery IAW RFC 1981 if routing functions are supported. (C)	5.3.5.4.1
54		Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (R)	5.3.5.4.1
55		Shall not use the Flow Label field as described in RFC 2460. (R)	5.3.5.4.2
56		Shall be capable of setting the Flow Label field when forwarding packets. (R)	5.3.5.4.2
57		Shall be capable of ignoring the Flow Label field when receiving packets. (R)	5.3.5.4.2
58		Shall support IPv6 addresses IAW RFC 4291. (R)	5.3.5.4.3
59		Shall support IPv6 scoped address IAW RFC 4007. (R)	5.3.5.4.3
60		If routing functions are supported: If DHCP is supported, the product shall support RFC 3315; if DHCPv6 is supported, it shall be implemented IAW RFC 3315. (C)	5.3.5.4.4
61	IPv6 Router Advertisements	If the system supports routing functions, the system shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements, and shall prefer routers that are reachable over routers whose reachability is suspect or unknown (C).	5.3.5.4.5.2
62		If the system supports routing functions, the system shall include the MTU value in the router advertisement message for all links IAW RFC 2461 and RFC 4861. (C)	
63		IPv6 Neighbor Discovery: The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	

Table 3-1. ASLAN Products CRs and FRs (continued)

ID	Requirement (See note.)		UCR 2008, Change 3 Reference
64	IPv6 Neighbor Discovery	If routing functions are supported: Neighbor discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5
65		The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
66		The system shall set the override flag bit in the neighbor advertisement message to “1” if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	
67	IPv6 SLAAC and Manual Address Assignment	If the system supports stateless IP address Auto-configuration, the system shall support IPv6 SLAAC for interfaces supporting UC functions IAW RFC 4862. (C)	5.3.5.4.6
68		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. (C)	
69		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the “managed address configuration” flag and the “other stateful configuration” flag to always be set and not perform stateless auto-configuration. (C)	
70		If the product supports stateless IP address auto-configuration including those provided for the commercial market, the DAD shall be disabled IAW RFC 4862. (C)	
71		The system shall support manual assignment of IPv6 addresses. (R)	
72		If the system provides routing functions, the system shall default to using the “managed address configuration” flag and the “other stateful flag” set to TRUE in their router advertisements when stateful auto-configuration is implemented. (C)	
73	IPv6 ICMP	The system shall support the ICMPv6 as described in RFC 4443. (R)	5.3.5.4.7
74		The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R)	
75		The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. (R) Required if LS supports routing functions.	
76		The system shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address (C). Required if LS supports routing functions.	
77		The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. (C) Required if LS supports routing functions.	
78	IPv6 Routing Functions	If the system supports routing functions, the system shall support the OSPF for IPv6, as described in RFC 5340. (C) This replaces RFC 2740.	5.3.5.4.8
79		If the system supports routing functions, the system shall support securing OSPF with IPsec as described for other IPsec instances in UCR 2008, Change 3, Section 5.4. (C)	
80		If the system supports routing functions, the system shall support OSPF for IPv6 as described in RFC 2740, router to router integrity using IP authentication header with HMAC-SHA1-128 with ESP and AH as described in RFC 4302 (IA superseding requirement), and shall support OSPFv3 IAW RFC 4552. (C)	
81		If the system supports routing functions, the system shall support the MLD process as described in RFC 2710 and extended in RFC 3810 and RFC 2711. (C)	
82	IPv6 Network Management	If nodes are managed via SNMP it shall use MIBs in conformance with RFC 4293. (R)	5.3.4.4.10/ 5.3.2.17.3.1.5
83		If the product performs routing functions and is managed by SNMP, the product shall support the IP Forwarding MIB as defined in RFC 4292. (R)	5.3.4.4.10
84	Site Requirements	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1
85		Wireless. (C)	5.3.1.7.2
86		Traffic Engineering. (R)	5.3.1.7.3
87		VLAN Design and configuration. (R)	5.3.1.7.4
88		Battery back-up 2 hours for non-ASLAN components and 8 hours for ASLAN components. (R) (Site requirement)	5.3.1.7.5
89		Availability of 99.999 percent (Special C2), and 99.997 percent (C2) for ASLAN (R), and 99.9 percent (non-C2 and C2(R) for non-ASLAN. (R) (Site requirement)	5.3.1.7.6

Table 3-1. ASLAN Products CRs and FRs (continued)

ID	Requirement (See note.)		UCR 2008, Change 3 Reference
90	IA Security Requirements	Port-Based Access Control IAW IEEE 802.1x. (R)	5.3.1.3.2
91		Secure methods for network configuration. SSH2 instead of Telnet and support RFCs 4251-4254. Must use HTTPS instead of HTTP, and support RFCs 2660 and 2818 for ASLAN and non-ASLAN. (R)	5.3.1.6
92		IPSec shall be IAW RFC 4301. (R if IPSec is supported)	5.3.1.3.8/ 5.3.5.4.9
93		Must meet IA requirements IAW UCR 2008, Change 3, Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5

NOTE: All requirements are for Core, Distribution, and Access layer components unless otherwise specified.

LEGEND:

AES	Advanced Encryption Standard	HTTP	Hypertext Transfer Protocol	MIB	Management Information Base
AH	Authentication Header			MLD	Multicast Listener Delivery
ANSI	American National Standards Institute	HTTPS	Hyper Text Transfer Protocol, Secure	MPLS	Multiprotocol Label Switching
ASLAN	Assured Services Local Area Network	IA	Information Assurance	ms	Millisecond
C	Conditional	IAW	In Accordance With	MTU	Maximum Transmission Unit
C2	Command and Control	ICMP	Internet Control Message Protocol	OSPF	Open Shortest Path First
C2(R)	Command and Control ROUTINE Only	ICMPv6	Internet Control Message Protocol for IPv6	OSPFv3	Open Shortest Path First Version 3
CB-WFQ	Class Based-Weighted Fair Queuing	ID	Identification	PHB	Per Hop Behavior
CPU	Central Processing Unit	IEEE	Institute of Electrical and Electronics Engineers	PQ	Priority Queuing
CQ	Custom Queuing	INCITS	InterNational Committee for Information Technology Standards	QoS	Quality of Service
DAD	Duplicate Address Detection			R	Required
DHCP	Dynamic Host Configuration Protocol	IP	Internet Protocol	RFC	Request for Comments
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPSec	Internet Protocol Security	SHA1	Secure Hash Algorithm Version 1.0
DISR	Department of Defense Information Technology Standards Registry	IPv4	Internet Protocol Version 4	SLAAC	Stateless Auto Address Configuration
DSCP	Differentiated Services Code Point	IPv6	Internet Protocol Version 6	SNMP	Simple Network Management Protocol
E2E	End-to-End	L2	Layer 2	SSH2	Secure Shell Version 2
ESP	Encapsulating Security Payload	L3	Layer 3	TCI	Tag Control Information
FIFO	First-in First-Out	LACP	Link Aggregation Control Protocol	TIA	Telecommunications Industry Association
Gbps	Gigabits Per Second	LAN	Local Area Network	UC	Unified Capabilities
HMAC	Hash-Based Message Authentication Code	LLDP	Link Layer Discovery Protocol	UCR	Unified Capabilities Requirements
		LS	LAN Switch	VLAN	Virtual Local Area Network
		Mbps	Megabits Per Second	VPN	Virtual Private Network
		MIB	Management Information Base	WFQ	Weighted Fair Queuing